



## Políticas y Procedimientos de Seguridad Informática Departamento de Educación de Puerto Rico

Recomendado por:

Fecha:

7 / AGO / 15

Ing. Maribel Picó Piereschi  
Oficial Principal de Informática

Aprobado por:

Fecha:

10 / ago / 15

Prof. Rafael Román Meléndez  
Secretario

**Tabla de contenido**

<b>I.</b>	<b>Introducción</b> .....	5
	Propósito .....	5
	Base legal .....	6
	Responsabilidades .....	6
	Recursos Humanos .....	6
	Vigencia de esta política y procedimiento de seguridad .....	6
<b>II.</b>	<b>Disposiciones generales de seguridad</b> .....	6
<b>III.</b>	<b>Responsabilidades del usuario</b> .....	9
	Queda prohibido .....	9
<b>IV.</b>	<b>Administrador de seguridad</b> .....	10
<b>V.</b>	<b>Planificación y aprobación de sistemas</b> .....	11
<b>VI.</b>	<b>Política de seguridad física</b> .....	11
	Categorías aplicables para acceso al Centro de Cómputos .....	12
	Personal autorizado .....	12
	Visitante .....	13
	Escolta .....	13
<b>VII.</b>	<b>Seguridad cibernética</b> .....	13
	<i>Firewall</i> .....	13
	<i>Antivirus</i> .....	13
<b>VIII.</b>	<b>Políticas de seguridad</b> .....	14
	Directorio .....	14
	Acceso al Internet .....	15
	Acceso remoto mediante <i>Virtual Private Network (VPN)</i> .....	15
	Cancelar permiso de VPN .....	16

Monitoreo del acceso y uso de los sistemas.....	16
Correo electrónico .....	16
Procedimiento de solicitud de cuentas de usuarios en el DE.....	17
Solicitud de cuenta .....	17
Asignación de permisos de administrador de las aplicaciones o sistemas.....	18
Procedimiento de creación de las cuentas por administrador de seguridad de las aplicaciones o sistemas.....	18
Correo electrónico.....	18
Recursos Humanos y Nómina (STAFF) .....	19
Sistema de Información Estudiantil (SIE) .....	19
Plan Comprensivo Escolar (PCEA).....	19
Mi Portal Escolar (MIPE).....	19
Tiempo, Asistencia y Licencia (TAL) .....	19
Administrador del Sistema de Información Financiera del DE (SIFDE) .....	19
Tarjeta de compras.....	19
<i>Configuration Manager / System Center</i> .....	19
Acceso remoto virtual .....	19
Internet .....	20
Cancelación de cuentas de usuarios en el DE.....	20
Mantenimiento de cuentas de usuarios en el DE.....	20
Revisión de personal con acceso.....	20
<b>IX. Formato de cuenta de usuario y clave de acceso.....</b>	<b>21</b>
Características para formato cuenta de usuario y contraseña .....	21
Periodo de expiración.....	22
<i>Account lockout</i> .....	22
Historial de contraseñas (password history) .....	22

	Cambio de clave.....	22
	Procedimientos y áreas de riesgo.....	22
	Registro y revisión de eventos.....	22
<b>X.</b>	<b>Disposición de equipos y licencias .....</b>	<b>22</b>
<b>XI.</b>	<b>Procedimiento de remoción de contenido .....</b>	<b>23</b>
	Proceso para recuperación de contenido .....	24
<b>XII.</b>	<b>Mantenimiento de equipos .....</b>	<b>24</b>
<b>XIII.</b>	<b>Plan de contingencias (en proceso de desarrollo) .....</b>	<b>24</b>
	Análisis de riesgos.....	25
	Prevención ante los desastres.....	25
	Actividades durante el desastre.....	26
	Continuidad de negocios .....	26
	Proceso de recuperación.....	27
	Documentación de los incidentes .....	27
<b>XIV.</b>	<b>Servicios profesionales o consultoría externa .....</b>	<b>27</b>
	Identificación de riesgos del acceso de terceras partes.....	28
	Contratos o acuerdos con terceros.....	28
	Requerimientos de seguridad en contratos de servicios profesionales o consultoría externa .....	30
<b>XV.</b>	<b>Definiciones.....</b>	<b>30</b>
<b>XVI.</b>	<b>Referencias.....</b>	<b>35</b>
	Anejos .....	36

## I. Introducción

- **Propósito**

La seguridad informática es un proceso de administración de los riesgos de los sistemas de información y los componentes integrados, que se apoya en políticas y procedimientos para atender las necesidades del Departamento de Educación de Puerto Rico (DE).

Las políticas y los procedimientos de seguridad informática tienen como objetivo proteger los activos físicos e intelectuales utilizados en la generación de información de la Oficina de Sistemas de Información y Apoyo Tecnológico a la Docencia (OSIATD). El Procedimiento de Seguridad Informática aplica al nivel central y a todas las áreas dentro del DE (escuelas, institutos tecnológicos y escuelas especializadas, escuelas para adultos y centros de exámenes libres, distritos, oficinas regionales, centros de servicios de educación especial, oficina central de comedores escolares, almacenes de alimentos y almacenes de equipo, centros de archivos inactivos, OMEP, imprenta y demás dependencias), ya sea por requerimiento o cuando se estime necesario por una operación relacionada o autorizada. Además, aplica a todo el personal de OSIATD, contratistas, consultores, personal temporero y todo aquel personal que utilice de manera directa o indirecta los sistemas de información, aplicaciones y plataformas del DE. El establecimiento de procedimientos y medidas de seguridad tiene como objetivo salvaguardar la Unidad Administrativa, el Centro de Cómputos, la División de Apoyo Tecnológico a las Escuelas, estructuras físicas, al personal, procedimientos operacionales, la información y la documentación generada, contra cualquier evento natural o humano que, de forma intencional o por accidente, puedan afectarlos.

Es responsabilidad de los usuarios cumplir con las políticas y procedimientos de seguridad informática. La falta de conocimiento de las políticas aquí descritas no libera al usuario de sanciones o penalidades por el incumplimiento de las mismas.

Todos los sistemas de tecnología que se utilicen como parte de la propiedad física o intelectual del DE se consideran protegidos por esta política y procedimiento de seguridad.

A tales efectos debemos tener como principios aplicables las siguientes premisas:

*Seguridad de Informática – “Protección de los sistemas de información en contra del acceso o modificación física o electrónica de la información; protección en contra de la negación de servicios a usuarios autorizados o de la disponibilidad de servicios a usuarios no autorizados; las políticas, normas, medidas, proceso y herramientas necesarias para detectar, documentar, prevenir y contrarrestar los ataques a la información o servicios antes descritos; los procesos y herramientas necesarias para la restauración de la información o los sistemas afectados por las brechas en la seguridad; disponibilidad y protección de los recursos requeridos para establecer dicha seguridad.” OGP TIG-003*

- **Base legal**

Ley núm. 151 del 22 de junio de 2004, conocida como Ley de Gobierno Electrónico, establece que la Oficina de Gerencia y Presupuesto tendrá la facultad para instrumentar, establecer y emitir la política pública a seguir y las guías que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales con el objetivo primordial de lograr la interconexión de los organismos para facilitar y agilizar los servicios al pueblo.

- **Responsabilidades**

Las políticas de seguridad informática y cualquier enmienda a las mismas deben ser aprobadas por el secretario de Educación y recomendadas por el oficial principal de informática (OPI), (*Chief Information Officer*) del DE. Las mismas son cónsonas con las políticas de la Oficina de Gerencia y Presupuesto del Estado Libre Asociado de Puerto Rico.

- **Recursos humanos**

OSIATD debe asegurarse de contar con el personal necesario, ya sea interno o contratado, para diseñar y mantener la seguridad de los sistemas de información.

Para el proceso de reclutamiento del personal de sistemas de información, especialmente para el área de seguridad, se debe llevar a cabo un proceso riguroso de selección del candidato para garantizar que, más allá de las credenciales académicas, en efecto tiene las destrezas tecnológicas necesarias para el puesto.

- **Vigencia de esta política y procedimiento de seguridad**

Debido a la evolución de la tecnología, las amenazas de seguridad y las nuevas tendencias, las políticas y los procedimientos incluidos en este documento se revisarán cada 2 años o según las necesidades del DE, para realizar actualizaciones y modificaciones necesarias. Esta política estará vigente a partir de su divulgación y hasta que la autoridad nominadora o el oficial principal de informática así lo determine.

Cambios a este procedimiento deben tener la aprobación del secretario de Educación y la recomendación del POI del DE. Los cambios realizados en esta política se divulgarán a todos los usuarios.

## II. **Disposiciones generales de seguridad**

Con el fin de establecer las políticas, los procedimientos y los requisitos para asegurar la seguridad informática para el DE, queda establecido que:

- ❖ El usuario no tendrá ninguna expectativa de intimidad con relación a la información almacenada en la computadora que tenga asignada o en cualquiera otra que utilice. Esto aplica a aquellas de propiedad del empleado y que, por voluntad y para beneficio de su propio desempeño, son autorizadas a conectarse a través de la red del Departamento y estarán sujetas a todas las auditorías y políticas de seguridad aquí contenidas. Además, estos equipos deben tener instalado un antivirus actualizado y autorizado.
- ❖ El DE se reserva el derecho de auditar, vigilar y fiscalizar los sistemas de correspondencia electrónica y todos los servicios computarizados para garantizar que los mismos se utilicen para las gestiones y los propósitos relacionados al trabajo. Estas auditorías se realizarán periódicamente, al azar o cuando exista una investigación sobre una situación en particular. Por estas circunstancias, el personal del DE no tiene derecho a la intimidad en relación con cualquier información, documento o mensaje creado, recibido o enviado por el sistema de correo electrónico, al usar las computadoras de la Agencia o algún equipo de carácter público o personal mediante el cual se acceda al servicio de correo electrónico del DE.
- ❖ Para salvaguardar la confidencialidad de la información del DE, no está permitido el envío fuera del Departamento de documentos electrónicos o mensajes por medio del correo electrónico que contengan información confidencial de la Agencia.
- ❖ Se podrán utilizar cuentas personales de servicios de correo electrónico y acceso a Internet (Hotmail, Gmail, Yahoo, entre otros) en los equipos del Departamento, siempre y cuando que se cumpla con los procedimientos establecidos. Sin embargo, se prohíbe modificar los privilegios de acceso a las redes internas o externas para obtener acceso a dichos recursos.
- ❖ Ningún usuario podrá modificar o asignar contraseñas, o modificar de manera alguna la información, mensajes de correo electrónico o archivos que son propiedad del DE, para lo siguiente:
  - ✓ Impedir que alguien pueda leerlos, entenderlos o utilizarlos
  - ✓ Falsificar o alterar el nombre del usuario
  - ✓ Falsificar o alterar la fecha de creación
  - ✓ Modificar información que se utilice para identificar documentación, mensajes o archivos.

En el caso de que, por razones de seguridad, se permita codificar, asignar contraseñas o modificar alguna información a fines de evitar que otras personas puedan leerlas, el DE estará facultado para decodificar la misma o restituirla a su condición original. El usuario será responsable de proveer todos los datos para lograr acceso a la información o el archivo.

La modificación de los parámetros o configuración de las computadoras del DE para ampliar las capacidades de la red del Departamento serán realizadas por personal asignado y autorizado

por OSIATD.

Los medios de almacenaje de información portátiles que sean utilizados en el DE deben ser revisados y certificados para garantizar que están libres de virus.

Todos los archivos que se creen en las computadoras se deben guardar en el directorio asignado y protegerse mediante los mecanismos de resguardo (*backup*) existentes.

Cada usuario es responsable de realizar un procedimiento de resguardo de la información archivada en su computadora una vez a la semana. OSIATD no será responsable del resguardo de documentos y archivos de los usuarios.

El DE cuenta con controles automáticos para la prevención y detección de programas no deseados (i.e. virus, *spyware*, *adware* y actualizaciones automáticas).

La seguridad de la información debe ser parte integral del diseño de cualquier programa de aplicación que se adquiera o se desarrolle en el DE para facilitar las operaciones de la agencia o mejorar el servicio a los ciudadanos. Es política de OSIATD que cada programa o aplicación pueda trabajar con los privilegios otorgados mediante el *Active Directory* y no mediante accesos creados única y exclusivamente para algún programa o aplicación específica.

La información y los programas de aplicación que se utilizan en las operaciones de la agencia tienen controles de acceso, de tal manera que solamente el personal autorizado pueda dar acceso a los datos y las aplicaciones (o módulo de la aplicación) que necesita utilizar. Estos controles incluyen mecanismos de autenticación y autorización (véase la sección de Definiciones).

Todos los mecanismos de autenticación deben incluir una contraseña combinada de números y letras mayúsculas, minúsculas y caracteres especiales tales como: @!#\$%^&\*()<>. Esta nomenclatura no será menor de seis (6) caracteres.

Los privilegios de acceso de los usuarios se reevalúan anualmente (Véase Sección VIII: **Mantenimiento de Cuentas de Usuarios en el DE**) o cuando el secretario o la autoridad delegada así lo disponga.

Las aplicaciones y los sistemas críticos o sensitivos (SIFDE, SIE, TAL y STAFF), que están instalados en los servidores que residen y operan en el Centro de Cómputos del DE, cuentan con la funcionalidad y capacidad de registrar y monitorear las actividades y transacciones de los usuarios.

La disposición o descarte de todo equipo que va a salir de la agencia y que contenga información sensitiva, debe seguir el proceso de remoción de datos y programas de forma segura para que los mismos no estén expuestos ni disponibles a personal no autorizado.

El DE cuenta con los programas o herramientas que configuran los controles necesarios para evitar que de forma intencionada o accidental se inicien ataques desde la red interna hacia sistemas de información externos y viceversa.

### III. Responsabilidades del usuario

Los recursos informáticos, datos, programación (*software*), redes y sistemas de comunicación electrónica están disponibles exclusivamente para realizar las funciones para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso. Los usuarios son responsables de toda actividad relacionada al uso de su acceso autorizado.

Los usuarios notificarán a su jefe inmediato sobre cualquier incidente que detecten que afecte o pueda afectar a la seguridad de los datos, o por sospecha de uso indebido del acceso autorizado por otras personas.

Todo usuario es responsable de proteger y no compartir su contraseña. En caso de que algún usuario piense que su contraseña ha sido descubierta, debe notificar al administrador de seguridad inmediatamente. El administrador de seguridad definirá una contraseña temporera, la cual será cambiada por el usuario.

El usuario o funcionario deberá reportar de forma inmediata cuando detecte algún riesgo real o potencial sobre equipos de computadoras o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas, golpes o peligro de incendio, entre otros. De igual forma, tiene la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad y que contengan información confidencial o importante.

Todo usuario que accede a los Sistemas de Información del DE debe utilizar únicamente las versiones de los programas autorizadas y siguiendo sus normas de utilización.

#### • **Queda prohibido**

- ❖ Instalar copias ilegales de cualquier programa, incluidos los estandarizados.
- ❖ Instalar cualquier dispositivo que altere la configuración actual de la red, entiéndase la instalación de: *routers*, *access points*, *switch*, *hubs*, impresoras, dispositivos alternos para conexión a Internet, entre otros.
- ❖ Destruir, alterar, inutilizar o dañar de cualquier otra forma los datos, programas o documentos electrónicos.

- ❖ Albergar datos de carácter personal en las unidades locales de disco de las computadoras de trabajo.
- ❖ Intentar obtener otros derechos o accesos distintos a aquellos que les han sido asignados.
- ❖ Intentar acceder a áreas restringidas de los sistemas de información o de la red, *software* o *hardware*, cuartos de telecomunicaciones, gabinetes de telecomunicaciones (caja negra) y centro de cómputos, entre otros.
- ❖ Intentar distorsionar o falsear los registros (*log*) de los sistemas de información.
- ❖ Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, ni dañar o alterar los recursos informáticos.
- ❖ Intentar utilizar las áreas y espacios físicos designados para las telecomunicaciones como almacén o área para guardar los efectos y materiales de limpieza. Las cajas y papeles acumulan humedad y polvo y se pueden incendiar fácilmente. Los detergentes emiten gases químicos que deterioran los cables y corroen los equipos.

#### IV. Administrador de seguridad

El oficial principal de informática (OPI) designa al administrador de seguridad informática del DE. La responsabilidad principal es definir, administrar y mantener las políticas y procedimientos de seguridad aquí expuestos, incluida su documentación.

El administrador de seguridad es responsable de:

- ❖ Mantener este documento actualizado.
- ❖ Investigar y documentar cualquier incidente, según sea necesario, en el Sistema de Boletas. (Véase Anejo 01).
- ❖ Mantener a todas las partes informadas de cualquier incidente o situación de seguridad que se presente. (secretario de Educación, OPI, director del centro de cómputos, personal de centro de llamadas, directora de la Oficina de Comunicaciones y comisionado de Seguridad, entre otros.)
- ❖ Establecer los términos razonables de respuesta para detectar, reportar y responder a incidentes de seguridad.
- ❖ Divulgar entre los empleados y contratistas los procedimientos de cómo informar los diferentes tipos de incidentes.

- ❖ Desarrollar procedimientos para que los cambios a la seguridad de los sistemas se realicen, sean documentados adecuadamente y estén almacenados en medio físico o electrónico de manera segura.
- ❖ Coordinar adiestramientos a la gerencia y a los supervisores de la agencia sobre los controles de seguridad, requerimientos y beneficios correspondientes.
- ❖ Adiestrar o coordinar adiestramiento para el personal de sistemas de información y telecomunicaciones sobre técnicas modernas de seguridad de sus áreas.
- ❖ Divulgar a todos los empleados los procedimientos de seguridad que les apliquen.

## V. Planificación y aprobación de sistemas

El OPI o el director del Centro de Cómputos efectuará el monitoreo de la utilización de los recursos de computación para analizar el comportamiento y funcionamiento, evaluar las necesidades de capacidad de los sistemas en operación y hacer proyecciones de futuras demandas. Esto tiene el propósito de garantizar un procesamiento y almacenamiento adecuado actual y futuro. Para ello se tomará en cuenta los requerimientos de crecimiento de los sistemas actuales y los de los sistemas a implantarse, así como las tendencias actuales y proyectadas en el procesamiento de la información del DE para el periodo estipulado de vida útil de cada componente. Asimismo, informará las necesidades detectadas a las autoridades competentes para la acción correspondiente y así evitar una potencial degradación de ejecutoria de los sistemas o plataformas que afecten la continuidad del procesamiento de los datos y las transacciones.

Además, recomendarán los criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, incluido el plan de pruebas necesarias, antes de su aprobación final.

## VI. Política de seguridad física

El Centro de Cómputos es un área de acceso restringido o controlado. El administrador de Seguridad o el director del Centro de Cómputos es responsable de administrar el acceso al centro. Solo personal autorizado podrá tener acceso a las instalaciones del mismo y al área de los servidores.

Con el objetivo de prevenir y evitar accesos no autorizados, daños en los equipos e interferencias en los procesos, y a su vez proteger el equipo de procesamiento de información crítica del DE, se establecieron las siguientes medidas o controles para el acceso físico al centro:

- ❖ El personal autorizado tendrá visible o disponible en todo momento su identificación oficial del DE, así como la tarjeta de acceso electrónico o el código de seguridad.

- Todo empleado tiene que tener la identificación oficial del DE. Para solicitud de la misma, el supervisor seguirá el procedimiento establecido por la Secretaría Auxiliar de Recursos Humanos para emitir tarjetas oficiales de identificación.
  - Para obtener la tarjeta de acceso electrónico o el código de seguridad, el personal deberá solicitar la misma al director del Centro de Cómputos.
  - ❖ Los visitantes serán escoltados en todo momento por personal de OSIATD designado para esas funciones (escolta), quien será responsable de que el visitante tenga una conducta adecuada y aceptable.
  - ❖ Todo visitante debe tener una justificación razonable para tener acceso al Centro de Cómputos.
  - ❖ Se requerirá una identificación a la persona que solicite entrada al Centro de Cómputos. El escolta verificará la misma y registrará la información en el Registro de Visitantes (Anejo 02). En el caso de visitantes externos, la identificación con foto se retendrá hasta que finalice la visita guiada al centro.
  - ❖ El Registro de Visitantes (Anejo 02) se utilizará como requisito mínimo para evidenciar y registrar la presencia del personal del DE o de los visitantes escoltados al Centro de Cómputos.
  - ❖ El escolta utilizará su mejor juicio para evaluar la justificación de la solicitud del acceso. En caso de duda consultará con el director de Seguridad, con el director del Centro de Cómputos o con el OPI.
- **Categorías aplicables para acceso al Centro de Cómputos**
    - A. Personal autorizado

Obtiene acceso al Centro de Cómputos, usando el privilegio que otorga la tarjeta de acceso o código de seguridad e identificación con foto visible. Debe firmar el Registro de Visitantes (Anejo 02).
    - B. Visitante

Obtiene el acceso al Centro de Cómputos escoltado por personal de OSIATD asignado a dichas funciones. Debe firmar el Registro de Visitantes (Anejo 02), entregar una identificación con foto para obtener la identificación de visitante y, en caso de ser necesario, recibirá autorización por escrito. Para esto, debe completar el formulario Autorización Acceso Área Restringida Centro de Cómputos (Anejo 03).
    - C. Escolta

Personal designado que acompañará al visitante del Centro de Cómputos. Es responsable de que se firme el Registro de Visitantes (Anejo 02), de que se cumpla con las medidas de seguridad y protección de los activos residentes en el

Centro de Cómputos, y que el visitante mantenga una conducta apropiada durante su visita.

## VII. Seguridad cibernética

Para asegurar que los recursos de los sistemas de información se utilizan de la manera adecuada y que el acceso a la información contenida solo sea accesible a las personas autorizadas, el DE cuenta con los mecanismos para proteger la confidencialidad, la integridad y la disponibilidad de los datos.

Además, existe un plan de contingencia para atender cualquier incidente en el cual se comprometa la seguridad y la disponibilidad de los datos y los sistemas. El DE cuenta con herramientas que garantizan la protección de los datos y los sistemas, tales como el *Firewall* y el antivirus.

- ***Firewall* (Protección de los sistemas y redes)**

La comunicación hacia el Internet se controla mediante la utilización de herramientas de protección conocidas como *Firewall* (véase Definiciones), y configuradas de acuerdo con un diseño de seguridad, según las recomendaciones y mejores prácticas del campo de seguridad cibernética y de acuerdo con recomendaciones y evaluaciones de la compañía *Gartner* (véase Definiciones). El DE cuenta con varios *Firewalls* para proteger los accesos autorizados y bloquear los no autorizados a las aplicaciones y los programas.

Para filtrar el acceso indebido a páginas no aceptables en la red de las escuelas, institutos tecnológicos y escuelas especializadas, escuelas para adultos y distritos se utiliza el programa de filtrado de contenido conocido como *Fortinet*.

Para el nivel central y las dependencias administrativas se utiliza el *Microsoft Threat Management Gateway* 2010.

- **Antivirus**

Como parte de las políticas de seguridad establecidas, toda computadora, *ya sea portátil, tableta o de escritorio* y servidor tendrá instalada la imagen de computadoras del DE. La imagen de computadoras contiene el programado básico (sistema operativo, MS Office, el antivirus y la política de uso aceptable del DE), el cual se actualiza cada 2 días.

El administrador de la red es responsable de remover cualquier virus detectado. Este incidente se debe documentar y comunicar a todos los usuarios inmediatamente por correo electrónico en comunicaciones oficiales, de ser necesario.

## VIII. Políticas de seguridad

### • Directorio

Los accesos a cada sistema se otorgan al usuario, de acuerdo con las funciones que tienen asignadas. Estos accesos tienen que ser aprobados por el supervisor inmediato. Así mismo, se llevará a cabo el procedimiento de cancelación de cuenta de usuario del DE (incluido como parte de este documento), cuando un empleado deja de ser empleado del Departamento por una de las siguientes razones:

- ✓ Licencia indefinida
- ✓ Renuncia
- ✓ Despido
- ✓ Jubilación
- ✓ Muerte
- ✓ Cancelación de contrato

Los privilegios de acceso de los usuarios se reevaluarán anualmente. El dominio en la red del DE (*Active Directory Server*), mantendrá activo por seis (6) meses el historial de seguridad; pasado este periodo, el historial se eliminará automáticamente.

Las cuentas de usuario permiten acceder a los siguientes programas o aplicaciones:

1. Correo electrónico
2. Recursos Humanos y Nómina (STAFF)
3. Red Informática Comedores Escolares (RICE)
4. Plan Comprensivo Escolar Auténtico (PCEA)
5. Plan Comprensivo Ocupacional Auténtico (PCOA)
6. Plan Comprensivo Escolar En Línea (PCEE)
7. Mi Portal Especial (MIPE)
8. Tiempo, Asistencia y Licencia (TAL)
9. Tarjeta de Compras
10. Acceso Remoto
11. Internet
12. Enterac

Las cuentas de usuario para acceder a los siguientes programas se realizan directamente en la aplicación, SIE y Office 365.

- **Acceso al Internet**

Los medios de redes de comunicaciones y computadoras personales para acceso a los servicios de Internet se proveen a aquellos empleados que requieran de esta para realizar las tareas y actividades en el desempeño de sus funciones. Todas las actividades en Internet deben estar relacionadas a las tareas y actividades en el desempeño de su trabajo. El Manual de Procedimientos para el Uso del Internet, correo electrónico y otros recursos de tecnología del DE, indican el uso adecuado, el no adecuado y las medidas disciplinarias en caso de incumplimiento.

Las políticas de acceso a Internet se revisan periódicamente. Se divulgarán y estarán disponibles para todo el personal y estudiantes del DE.

- **Acceso remoto mediante *Virtual Private Network (VPN)***

El director de área o supervisor inmediato es responsable de solicitar el servicio de acceso remoto y el OPI o el director del Centro de Cómputos es responsable de autorizar dicho acceso.

Cualquier equipo del DE utilizado fuera de la agencia debe ser autorizado por el director de cada área o supervisor inmediato. Este será responsable de que el usuario cumpla con los procedimientos de utilización adecuada de los equipos fuera de la agencia.

Para que un usuario o consultor del DE pueda acceder a los equipos, ya sean servidores u otros equipos de la red interna del DE desde una conexión externa con la tecnología VPN, cumplirá con el siguiente procedimiento:

1. El supervisor del usuario o consultor solicitará por medio del Formulario de Creación de Cuenta de Usuario (Anejo 05) el acceso remoto mediante el servicio de VPN.
2. En la solicitud incluirá la justificación para la solicitud de este acceso e indicará el tiempo requerido para el mismo y para aprobar la solicitud para el usuario o consultor. Esto aplica a personal que tiene que realizar tareas fuera de horas laborables o en instalaciones que necesiten este tipo de acceso, participar en proyectos que requieran apoyo remoto, o alguna otra circunstancia especial que así lo amerite.
3. El OPI o el director del Centro de Cómputos evalúa la solicitud; si aprueba la misma, se refiere al personal designado para procesar el permiso y acceso VPN. De no aprobar la misma, se devuelve al supervisor o contratista con las razones de la decisión.
4. Una vez procesado el permiso, se notifica al usuario o consultor y se le dan las instrucciones para conectarse vía VPN. Si es necesario, personal técnico asistirá al usuario en el proceso de configurar el VPN.

- **Cancelar permiso de VPN**

Para eliminar el permiso de VPN de un usuario o consultor, el supervisor enviará un correo electrónico al OPI o al Director de Centro de Cómputos para solicitar la cancelación del permiso. Esta solicitud se refiere al personal designado para que procedan con la cancelación del permiso.

En caso de que la solicitud inicial indique que es un permiso temporero o por un tiempo determinado, el acceso se deshabilitará o cancelará el día siguiente de la fecha indicada.

Cuando se desactiva el acceso de un usuario a la red, automáticamente se desactivan los permisos de VPN.

- **Monitoreo del acceso y uso de los sistemas**

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. Los registros de auditoría deberán incluir la identificación del usuario, la fecha y hora de inicio y terminación, así como la identidad y ubicación del equipo. Además, debe incluir un registro de intentos exitosos y fallidos de acceso a los sistemas, datos y otros recursos de tecnología.

- **Correo electrónico**

Las cuentas de correo electrónico oficiales provistas por el DE son para propósitos exclusivos de las funciones oficiales. A continuación, se detalla el uso no adecuado del correo electrónico:

- ❖ Está prohibido revisar, leer o interceptar cualquier tipo de comunicación electrónica del DE, o de cualquier otra persona o entidad, sin el consentimiento expreso del remitente y del destinatario de la comunicación.
- ❖ El usuario se abstendrá de suscribirse a listas de correo electrónico o de participar en grupos noticiosos (*newsgroups*) que divulguen información o mensajes ajenos a las funciones y deberes del DE.
- ❖ Existe una prohibición absoluta (cero tolerancia) a la utilización de la computadora o del sistema de correspondencia electrónica para enviar, recibir o crear mensajes en cadena y mensajes o documentos de contenido discriminatorio de ninguna manera por razón de edad, raza, color, sexo, nacimiento, condición de veterano, ideología política o religiosa, origen o condición social, orientación sexual o identidad de género, discapacidad o impedimento físico o mental; ni por ser víctima de violencia doméstica, agresión sexual o acecho.
- ❖ Está prohibido el manejo o transmisión de material obsceno, profano u ofensivo por medio del sistema de computadoras o del sistema de comunicación electrónica del DE. Esto incluye el acceso a materiales eróticos, broma de cualquier forma o cualquier comentario o chiste que pueda violar la política de discriminación, *bullying*, *cyberbullying* o política de hostigamiento sexual, entre otros.

- ❖ El usuario se abstendrá de enviar, vía correo electrónico, archivos que excedan la capacidad de la cuota asignada.

Las políticas antes mencionadas sobre el uso del correo electrónico y auditorías de uso y registro, tendrán igual aplicación para los otros servicios o funciones disponibles en Intranet e Internet, tales como FTP y Chat, (véase Definiciones), entre otros.

- **Procedimiento de solicitud de cuentas de usuarios en el DE**

Para todo usuario nuevo, se notificará a OSIATD para asignarle los derechos correspondientes, (creación de usuario para la Red, perfil de usuario en el directorio activo, entre otros) o en caso de retiro del funcionario, anular y cancelar los derechos otorgados como usuario.

- **Solicitud de la cuenta:**

1. El usuario solicita la cuenta de acceso al DE por medio del Formulario de Creación de Cuenta de Usuarios (anejo 05). Los accesos al SIE o SIFDE se solicitan directamente a la oficina que administra estos sistemas (anejo 06).
2. El formulario debe ser completado en todas sus partes; esto incluye la firma del solicitante y su supervisor. Si el acceso tiene fecha de vencimiento, el supervisor debe indicar el periodo en el Formulario Autorización de Cuenta de Usuario (anejo 5) de manera que el sistema desactive automáticamente en dicha fecha.
3. Envía el formulario al Centro de Cómputos, ubicado en el 4.º piso de la antigua sede del DE. Puede enviarse por fax al 787-767-6935 o por correo electrónico a la siguiente dirección: [helpdesk@de.gobierno.pr](mailto:helpdesk@de.gobierno.pr)
4. Una vez se crea la cuenta, se envía la información del “*username*” y “*password*” al usuario y se le informa. Mediante la creación de una boleta de servicio se asigna al área de Apoyo Técnico para que proceda a configurar la cuenta de usuario en la computadora, de ser necesario. Es responsabilidad de cada departamento u oficina solicitar que se verifique previamente el equipo de computadora que se va a asignar a los empleados.

- **Asignación de permisos de administrador de las aplicaciones o sistemas.**

La solicitud de este permiso está incluido en el Formulario de Autorización de Cuenta de Usuario (anejo 05) y debe ser autorizada y justificada por el director de área o supervisor inmediato y por el OPI o el director del Centro de Cómputos. El permiso de administrador en los servidores se otorga a usuarios con las siguientes características:

- ❖ Administradores de OSIATD (administrador del sistema de correo electrónico, administrador de *Active Directory*, administrador de SQL (bases de datos, entre otros) que, por la naturaleza de las funciones de su trabajo, requieran tener acceso a los servidores para dar mantenimiento y realizar configuraciones en los mismos.
- ❖ Operadores que, por la naturaleza de sus funciones de trabajo, requieran tener acceso a los servidores para ejecutar procesos de mantenimiento u otros procesos necesarios.
- ❖ Consultores contratados para dar mantenimiento y realizar configuraciones en servidores de aplicaciones.
- ❖ Consultores contratados para asistir en el mantenimiento de los servidores.
- ❖ Consultores contratados para desarrollar una aplicación o realizar mejoras a una existente y que requieran acceso a los servidores donde residen las mismas.

El permiso de administrador en equipos (computadoras personales, tabletas y portátiles) del DE se otorga a:

- ❖ Técnicos del DE que ofrecen apoyo técnico en la configuración y el mantenimiento de los equipos, programas y dispositivos de los usuarios.
  - ❖ Consultores que ofrecen apoyo técnico en la configuración y el mantenimiento de los equipos, programas y dispositivos de los usuarios.
  - ❖ Excepciones para dar este permiso a otro personal no mencionado tiene que ser aprobado por el OPI.
- **Procedimiento de creación de las cuentas por administrador de seguridad de las aplicaciones o sistemas.**
    - A. Correo electrónico
      - Una vez se crea la cuenta del usuario, se asigna una cuenta de correo electrónico, El supervisor de cada empleado debe autorizar y justificar este acceso en la solicitud.
    - B. Recursos Humanos y Nómina (STAFF)
      - Los permisos de STAFF son aprobados y solicitados por la Secretaría Auxiliar de Recursos Humanos.
    - C. Sistema de Información Estudiantil (SIE)
      - Según las Políticas para la Administración del Sistema de Información Estudiantil (SIE) y las Políticas para la Creación de Cuentas de Usuarios para el Portal de Padres, estas cuentas se crean por personal designado.

D. Plan Comprensivo Escolar Auténtico (PCEA)

Utiliza el mismo *user* y *password* de la cuenta del DE (*Active Directory*). No requiere una cuenta adicional. Para las escuelas nuevas, se añade al grupo correspondiente en el PCEA.

E. Mi Portal Escolar (MIPE)

La creación de cuentas las trabaja el personal técnico o designado de la Secretaría Asociada de Educación Especial, con el formulario correspondiente.

F. Tiempo, Asistencia y Licencia (TAL)

La creación de estas cuentas las trabaja el personal técnico o designado de la Secretaría Auxiliar de Recursos Humanos.

G. Administrador del Sistema de Información Financiera del DE (SIFDE)

El administrador de este sistema envía los formularios de creación de cuentas de los usuarios al Centro de Cómputos, una vez el usuario haya tomado sus talleres y adiestramientos. Se crean las cuentas de acceso a la red en el *Active Directory* y se devuelven al administrador del SIFDE para que creen la cuenta al usar como base la creada para acceder la red del DE.

H. Tarjeta de compras

El administrador de Sistema de Tarjeta de Compras envía el formulario de petición de cuenta de usuarios al Centro de Cómputos. Solo a aquellos usuarios que han tomado el adiestramiento y tienen en su poder físicamente la tarjeta se les crea la cuenta. Una vez se crea la cuenta se informa al administrador.

I. *Configuration Manager / System Center*

Utiliza la cuenta del *Active Directory* como base y se otorgan los privilegios de acuerdo con las indicaciones aprobadas por el supervisor inmediato del usuario. (Para uso exclusivo de OSIATD).

J. Acceso Remoto Virtual (VPN)

El supervisor del área indica en el Formulario de Solicitud Acceso (Anejo 05) y la necesidad y justificación de este servicio. Una vez aprobada, se añaden los privilegios a la cuenta del usuario.

K. Internet

El supervisor del área indica en el Formulario de Solicitud de Acceso (Anejo 05) y autoriza el acceso a este servicio. Cuando se crea la cuenta, se asignan los permisos de acceso al Internet.

Para todos estos programas o servicios, una vez se crea la cuenta y, si no hay algún otro proceso pendiente, se archiva el documento y se le informa al que solicitó la cuenta. De ser necesario, el usuario solicita apoyo para configurar su computadora, se comunica al 787-773-3076, para registrar la petición en el sistema de boletas y se asigna un técnico de la Unidad de Apoyo Técnico.

Las cuentas para personal docente y estudiantes está disponible en Office 365, también conocido como @miescuela.pr (véase Anejo 09).

- **Cancelación de cuentas de usuarios en el DE**

La Secretaría Auxiliar de Recursos Humanos envía diariamente a OSIATD un informe de los empleados con estatus de TERMINADO según el Sistema STAFF, con el propósito de eliminar los accesos que tengan a los sistemas de información. Recursos Humanos trabaja en el diseño y desarrollo de un informe electrónico de empleados con estatus TERMINADO para que OSIATD lo reciba y procese todos los días.

El personal a cargo del mantenimiento de cuentas procede a cancelar los accesos de acuerdo con los siguientes pasos:

1. Deshabilita la cuenta.
2. Borra el buzón de correo (los mensajes permanecen durante 30 días, luego de borrarse, dentro de los servidores de correo electrónico), a menos que se solicite mantener por más tiempo. En los casos de licencia sin sueldo, la cuenta se mantiene deshabilitada por un año. En los demás casos, por 90 días.
3. Notifica a la Secretaría Auxiliar de Recursos Humanos que se procedió a deshabilitar la cuenta.

- **Mantenimiento de cuentas de usuarios en el DE**

- ❖ Revisión de Personal con Acceso

Anualmente, el día 1.º de abril, OSIATD generará una lista de usuarios activos con los accesos otorgados (Informe de Usuarios Autorizados, Anejo 07) que se enviará a los directores de área para su revisión y actualización. Una vez identifique el estatus de los usuarios y accesos, enviará a director del Centro de Cómputos para la acción correspondiente.

El director del Centro de Cómputos refiere al personal designado el informe con el estatus (modificar, desactivar, actualizar, entre otros), para el proceso correspondiente.

## IX. Formato de cuenta de usuario y clave de acceso

- Política de contraseñas (*Password*)

El DE utiliza la técnica de autenticación (véase sección XXI, Definiciones) para proteger los accesos directo y remoto a la red local. La autenticación en el sistema de seguridad está compuesta de una cuenta de usuario y de una contraseña, la cual no impedirá que se audite el sistema en caso que sea necesario.

- **Características para formato cuenta de usuario y contraseña**  
(*Username & Password*)

1. La cuenta de usuario se definirá con la siguiente nomenclatura:

1.<sup>er</sup> apellido, 1.<sup>a</sup> letra del 2.<sup>o</sup> apellido, 1.<sup>a</sup> letra del nombre

Ej.: Juan López Muñiz → lopezmi

Si tiene un segundo nombre, se añade la inicial del segundo nombre al final.

Ej.: Juan C. López Muñiz → lopezmic

2. El *password* o contraseña estará compuesto por un mínimo de 6 caracteres y de una combinación de:

1. Letras mayúsculas
2. Letras minúsculas
3. Caracteres especiales como @!#\$%^&\*()<>
4. Números

Ej.: MLJwerty<@6521>

3. La primera vez que el usuario acceda a la Red, tendrá que completar un proceso de cambio de contraseña.

- **Periodo de expiración**

El tiempo de expiración de la cuenta es dos (2) meses.

- **Account lockout**

Luego de 10 intentos fallidos de entrar a la cuenta, el sistema deshabilita la cuenta temporaneamente. Para reiniciarla, el usuario se tiene que comunicar con el Centro de Llamadas al 787-773-3076 o puede esperar aproximadamente 10 minutos para intentar reingresar.

- **Historial de contraseñas (*password history*)**

Para *Active Directory* y *Exchange*, el sistema mantiene las últimas 24 contraseñas definidas.

- **Cambio de clave**

Se requerirá que los usuarios realicen un cambio en su contraseña cada 60 días y no podrá utilizar las últimas 24 contraseñas registradas en el historial de contraseñas (*Password History*).

- **Procedimientos y áreas de riesgo**

OSIATD monitoreará el uso de los sistemas de información para garantizar que los usuarios solo estén realizando actividades autorizadas. Los responsables (dueños) de los sistemas de información indicarán los eventos que consideren críticos en la operación de los sistemas que requieran el registro de los mismos.

- **Registro y revisión de eventos**

Se implementará un procedimiento de revisión de los registros de auditoría, enfocado a producir un informe de las amenazas detectadas contra los sistemas y los métodos utilizados. Los dueños de los sistemas determinarán la periodicidad de las revisiones, de acuerdo con la evaluación de los riesgos y la probabilidad de ocurrencia.

## X. **Disposición de equipos y licencias**

Para disponer de equipos y licencias, cada unidad de trabajo llevará el proceso de acuerdo con el Procedimiento de Disposición de Equipo. Antes de disponer los mismos, se debe realizar el proceso de remoción de los programas, archivos y datos almacenados. Si el equipo contiene programas con licencias que no se reinstalarán en otro equipo, se notifica al personal a cargo del inventario de las mismas, para así mantener actualizado su información.

## XI. **Procedimiento de remoción de contenido**

Personal autorizado de OSIATD preparará una boleta para registrar la solicitud de remoción de contenido de acuerdo con el siguiente proceso:

1. Seleccionar el método de remoción más adecuado.
2. Mantener un registro de la información del equipo al que se le removió su contenido. Esto incluye:
  - a. Fecha en que se removió el contenido

- b. Número de serie del equipo
  - c. Marca y modelo
  - d. Método de remoción o destrucción utilizado
  - e. Nombre de la persona que hizo el proceso de remoción
  - f. Firma de la persona que hizo el proceso de remoción
3. Entregar las licencias que contenía el equipo. La política de Manejo de Licencias de Tecnología establece que se debe devolver las licencias que no están en uso. En el caso de las licencias globales adquiridas por OGP y que le pertenecen, se notificará una vez se finalice el proceso de remoción de contenido del equipo. Si los programas instalados en el equipo se van a utilizar en otro equipo, no procede el proceso de devolución.
  4. Transferir a otra entidad gubernamental el equipo que no se utilizará, luego de la remoción de su contenido. Si se dispone de equipo porque no cumple con las necesidades de esta entidad, división o unidad de trabajo, ya sea por capacidad, incompatibilidad u obsolescencia, pero se entiende que puede ser útil a cualquier otra, el mismo se entregará al oficial de propiedad para que la transfiera. Antes de dicha transferencia, el personal de OSIATD debe certificar que el equipo está en condiciones aceptables para utilizarse en otra oficina, departamento o cualquier otra dependencia del DE.
  5. Donar el equipo a escuelas o entidades sin fines de lucro, luego de la remoción de su contenido. Si se dispone de equipo porque no cumple con las necesidades de esta entidad, división o unidad de trabajo, ya sea por capacidad, incompatibilidad u obsolescencia, pero se entiende que puede ser útil a cualquier otra, el mismo se entregará al oficial de propiedad para que la transfiera. Antes de dicha transferencia, el personal de OSIATD debe certificar que el equipo está en condiciones aceptables para utilizarse en una escuela o coordinar con personal técnico de la entidad sin fines de lucro para verificar esta información.
  6. Decomisar el equipo que ya no se utilizará, luego de la remoción de su contenido. Si se está disponiendo del equipo porque es obsoleto y no cumple con los criterios anteriores, se llevará a cabo el proceso pertinente para decomisar dicho equipo, conforme a la reglamentación de Propiedad Excedente Estatal de la Administración de Servicios Generales.

- **Proceso para recuperación de contenido**

Para la recuperación de contenido a nivel de computadoras personales, el usuario accederá la aplicación y en el menú escogerá la opción de *file*, donde encontrará la lista de los últimos archivos creados o editados con dicha aplicación.

En el caso de recuperación de programas de computadora, el usuario deberá comunicarse con el administrador del sistema o el *Help Desk* de OSIATD para solicitar apoyo técnico.

Para la recuperación de correos electrónicos el usuario verificará en el folder de *Deleted Items*, en *Personal Folder*. Otra alternativa es activar la opción de búsqueda en *Microsoft Outlook*.

## **XII. Mantenimiento de equipos**

El mantenimiento y la reparación de los equipos de computadora y otros equipos o periferales tienen el objetivo de asegurar su disponibilidad y procesamiento óptimo, teniendo en cuenta lo siguiente:

- a. Las tareas de mantenimiento preventivo o ventanas de mantenimiento (véase Definiciones), se realizarán de acuerdo con los intervalos de servicio y especificaciones recomendadas por el proveedor.
- b. Solo el personal de autorizado puede brindar mantenimiento y realizar reparaciones.
- c. El mantenimiento preventivo y correctivo, y la detección de fallas se registran en el formulario *Request for Change* (Anejo 08).

## **XIII. Plan de contingencias (en proceso de desarrollo)**

Un Plan de Contingencias se basa en el análisis de los posibles riesgos a los cuales se está expuesto, tanto el equipo de tecnología, como la información contenida en los diversos medios de almacenamiento electrónico. El objetivo principal del plan es la restauración del servicio de forma rápida, eficiente y con el menor costo y pérdidas posibles.

- **Análisis de riesgos**

Para realizar el análisis de riesgo, es necesario un inventario de los activos de los sistemas de información que incluya el equipo, los programas y los datos. Todos los activos se clasifican de acuerdo con el nivel de importancia para la continuidad de las operaciones. Los datos se clasifican de acuerdo con su nivel de confidencialidad. Con esto se establecen los activos, la información que se protegerá y las prioridades.

Es necesario identificar las posibles amenazas contra los sistemas de información, el análisis del impacto en las operaciones y la probabilidad de que ocurran las mismas. A continuación la lista de las amenazas más comunes:

- ✓ Catástrofes

- ✓ Fuego
- ✓ Fallas de energía
- ✓ Ataques terroristas
- ✓ Interrupciones organizadas o deliberadas
- ✓ Sistema o fallas de equipo
- ✓ Error humano
- ✓ Virus informáticos
- ✓ Cuestiones legales
- ✓ Huelgas de empleados
- ✓ Eventos de la naturaleza

- **Prevención ante los desastres**

Con el propósito de establecer las mejores prácticas y salvaguardar la infraestructura tecnológica e informática, se deben realizar las siguientes actividades o tareas:

- ❖ Enviar resguardos fuera de la agencia diariamente para garantizar la disponibilidad de los datos de al menos un día antes de ocurrir cualquier evento.
- ❖ Incluir el *software*, así como toda la información de datos, para facilitar la recuperación.
- ❖ Usar una instalación remota de resguardo para reducir al mínimo la pérdida de datos.
- ❖ Contar con redes de Área de Almacenamiento (SAN) en múltiples sitios para que los datos estén disponibles inmediatamente sin la necesidad de llevar a cabo el proceso de recuperarlos (opcional).
- ❖ Utilizar protectores de línea (UPS) para reducir al mínimo el efecto de fluctuaciones del servicio de energía eléctrica sobre un equipo electrónico sensible.
- ❖ Contar con un generador eléctrico con la capacidad necesaria para la continuidad de los servicios (SAI). Es importante que se realicen pruebas periódicas para asegurar el funcionamiento del mismo.
- ❖ Instalar alarmas y extintores accesibles tal como SM200, entre otros, para la prevención de incendios.

- **Actividades durante el desastre**

Una vez se declara la contingencia, la falla o el siniestro, se ejecutarán las siguientes actividades, definidas en el Plan de Emergencias:

- El plan establece las acciones que se realizarán cuando se presente una falla o un desastre, así como la coordinación y comunicación de las mismas. Es conveniente prever los posibles

escenarios de ocurrencia del siniestro, el cual se puede dar tanto en horario diurno, como nocturno.

- El plan debe incluir la participación y las actividades que realizarán por todas las personas asignadas al mismo o que puedan estar presentes en el área. Se tiene que identificar las salidas de emergencia y las vías de evacuación, la ubicación de los extintores, linternas y las lámparas de mano, los números telefónicos de emergencia y los nombres de funcionarios para contactar con los números de los proveedores de servicios.

- **Continuidad de negocios**

El Análisis de Riesgo mencionado sirve de base para el desarrollo de un Plan de Continuidad de Negocios que incluye un Plan para Recuperación de Desastres y un Plan para la Continuidad de las Operaciones. Este plan tiene los siguientes componentes:

1. Directorio telefónico de empleados- Se debe contar con un directorio telefónico actualizado. Cuando sea necesario, se notificará a todo el personal clave sobre la situación y se les asignarán tareas enfocadas hacia el plan de recuperación. Esta comunicación puede ser mediante un *Broadcast*, mensaje de texto en blog o individual, u otro medio efectivo.
2. Clientes- En caso necesario, se notificará a los clientes internos y externos sobre la situación. Se pueden utilizar los medios masivos de comunicación (radio, televisión, prensa escrita e Internet). Para estos fines, se coordina con la Oficina de Comunicaciones para que preparen el comunicado de prensa y determinen el medio que se utilizará.
3. Instalaciones- Tener un lugar establecido y preparado para relocalizar al personal asignado. Durante un desastre, a los empleados se les requerirá trabajar por periodos extensos y agotadores. Debe haber un plan de apoyo para aliviar un poco la tensión. Este debe incluir: lugar para descanso, alimentos, relevo de personal, medicamentos básicos y facilidad de comunicación con familiares, entre otros.
4. Procedimiento de resguardo- Es necesario contar con un procedimiento para llevar a cabo y mantener una copia de resguardo (*backup*) recurrente de la información y de los programas de aplicación y de los sistemas esenciales e importantes para la continuidad de las operaciones.
5. Centro de Cómputos- Las instalaciones donde residen los sistemas de información deberán estar localizadas en un área donde sea menor la probabilidad de daños por fuego, inundaciones, explosiones, disturbios civiles y otros desastres.

6. Centro alternativo- En caso de tener que restaurar los sistemas, se debe contar con un centro alternativo que permita los accesos a los sistemas críticos del DE. Este centro debe contar con acceso al Internet.

- **Procesos de recuperación**

Dependiendo de las consecuencias del incidente, se deberá realizar alguna de las siguientes actividades:

- ❖ Comprar equipo nuevo (*hardware*) o reparar el existente.
- ❖ Solicitar que el proveedor de *software* provea uno nuevo para instalarlo.
- ❖ Recuperar los discos de almacenaje.
- ❖ Reinstalar los datos y los sistemas.
- ❖ Restaurar los datos

- **Documentación de los incidentes**

En el sistema de boletas se documenta, cuantifica y monitorea los tipos de incidentes, la frecuencia, el impacto y los costos asociados a los mismos. Esta información se utiliza para identificar aquellos recurrentes o de alto impacto y evaluar mejoras o controles adicionales para limitar la frecuencia, los daños y los costos asociados a estos casos en el futuro.

#### **XIV. Servicios profesionales o consultoría externa**

La seguridad de los sistemas de información, aun cuando el manejo y el control de parte o de todos los procesos sean delegados a un tercero, es responsabilidad del DE.

Los contratos de servicio o profesionales con terceros deben incluir el salvaguardar los sistemas, los datos o equipos sensitivos, ya sean físicos o intelectuales, especialmente cuando los servicios contratados incluyen el manejo de estos fuera de las instalaciones del DE.

- **Identificación de riesgos del acceso de terceras partes**

Cuando exista la necesidad de otorgar acceso a terceras partes a información del DE, se llevará a cabo una evaluación de riesgos para determinar los requerimientos de controles específicos, teniendo en cuenta lo siguiente:

- ❖ El tipo de acceso requerido (físico/lógico y los recursos específicos).
- ❖ La justificación para el acceso.
- ❖ El valor de la información.
- ❖ Los controles implantados por la tercera parte.
- ❖ El efecto, si alguno, de este acceso en la seguridad de la información del DE.

Para los servicios ofrecidos por contratistas que son realizados fuera de los predios del DE, es necesario que se firme un acuerdo entre ambas partes. En todos los contratos se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso y los permisos que se otorgarán, sin que se afecte el servicio contratado. Todo contrato debe contener una cláusula de confidencialidad a tales efectos.

En ningún caso se otorgará acceso a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos a terceros, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

- **Contratos o acuerdos con terceros**

Para los contratos o acuerdos existentes o que se efectúen con terceros, se deben determinar si aplican los siguientes controles:

1. Cumplimiento de la Política de Seguridad del DE.
2. Protección de los activos del DE, que incluyen:
  - a. Procedimientos para proteger los bienes del DE, incluidos los activos físicos, la información y el *software*.
  - b. Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
  - c. Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en el momento convenido durante la vigencia del mismo.
  - d. Restricciones a copiar y divulgar la información.
3. Descripción de los servicios disponibles.
4. Nivel de servicio esperado y niveles de servicio aceptables (*Service Level Agreement*, o SLA).
5. Permiso para la transferencia de conocimiento al personal, cuando sea necesario.
6. Obligaciones de las partes de acuerdo con el contrato y las responsabilidades legales.
7. Existencia de derechos de propiedad intelectual.
8. Definiciones relacionadas a la protección de datos.
9. Acuerdos de control de accesos que incluyan:

- a. Métodos de acceso permitidos, y el control y uso de método de autenticación tal como la cuenta del usuario y las contraseñas de usuarios.
  - b. Proceso de autorización de accesos y privilegios de usuarios.
  - c. Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que van a implementar y los derechos y privilegios.
10. Definición de criterios de desempeño medibles, de monitoreo y de presentación de informes.
  11. Derecho a auditar las responsabilidades contractuales o establecidas en el acuerdo.
  12. Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones en relación con situaciones de contingencia.
  13. Responsabilidades relativas a la instalación y al mantenimiento de *hardware* y *software*.
  14. Estructura de la dependencia y del proceso de elaboración y presentación de informes que incluya un acuerdo con respecto a los formatos de los mismos.
  15. Proceso claro y detallado de administración de cambios.
  16. Controles requeridos de protección física y los mecanismos que aseguren la implementación de los mismos.
  17. Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
  18. Controles que garanticen la protección contra *software* malicioso.
  19. Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativas a la seguridad.
  20. Relación entre proveedores y subcontratistas.

- **Requerimientos de seguridad en contratos de servicios profesionales o consultoría externa**

Los contratos o acuerdos de Servicios Profesionales o Consultoría Externa total o parcial para la administración y control de sistemas de información, redes y/o ambientes de computadoras personales del DE incluirán, además de los puntos especificados en la Sección de Contratos o Acuerdos con Terceros, los siguientes:

1. Forma en que se cumplirán los requisitos legales aplicables.
2. Medios para garantizar que todas las partes involucradas en la tercerización, incluidos los subcontratistas, conocen sus responsabilidades sobre la seguridad cibernética.

3. Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos del DE.
4. Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible del organismo.
5. Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
6. Niveles de seguridad física que se asignarán al equipo de externos.
7. Derecho a una auditoría por parte del DE en forma directa o mediante la contratación de servicios.

Se debe prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes.

## XV. Definiciones

**Active Directory** - Servicio de directorio en la red distribuida de computadoras.

**Access points** - centro de comunicación para los usuarios, de un dispositivo inalámbrico, para conectarse a una cableada LAN. Son importantes para ofrecer mejor seguridad inalámbrica y para ampliar la cobertura de servicio del usuario.

**Adware** - Es un programa que se instala inadvertidamente en una computadora y su principal propósito es desplegar ante el usuario anuncios y propaganda, pero también puede tener un comportamiento como el *spyware* (véase *Spyware*).

**Antivirus** - programa que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema para evitar robo y pérdida de información, alteración del funcionamiento, disrupción del sistema y propagación hacia otras computadoras.

**Autenticación** - Es el proceso por el cual una persona presenta información que lo identifica ante un sistema de información con el propósito obtener acceso; el sistema compara la información contra su base de datos para validar que es un usuario autorizado.

**Autorización** - Es el proceso por el cual se adjudican privilegios específicos a una persona para el uso de recursos en los sistemas de información.

**Comunicación externa** – Toda aquella comunicación fuera de la red del DE y sus dependencias.

**Confidencialidad** - Es la característica que se le da a una información para que pueda ser vista solamente por personas autorizadas.

**Continuidad del negocio** - Es un concepto que abarca tanto la Planeación para Recuperación de Desastres (DRP) como la Planeación para el Restablecimiento del Negocio.

**Datos sensitivos** - Datos que contienen información financiera, de los ciudadanos, de los recursos humanos u otra información crítica para la operación de la agencia.

**Disposición de equipo** - Proceso de eliminar equipo perteneciente a la agencia. El proceso de eliminar puede implicar el transferir el equipo a otra oficina u agencia, donarlo a una entidad sin fines de lucro o decomisarlo.

**Empleado terminado** – empleado que ya no trabaja para el Departamento de Educación.

**Encriptación** - Proceso por el cual unos datos se transforman en información no entendible por aquellos que no están autorizados a verlos.

**Equipo** - Incluye, pero no se limita a: computadoras, impresoras, cables, *hubs*, *routers*, *switches*, servidores, *access points*, baterías (UPS), escáneres y demás accesorios.

**Firewall (equipo de seguridad de computadoras y redes)** - Aplicación, equipo o conjunto de ambos, que protege los recursos de la red de accesos no autorizados. En el caso de las aplicaciones, son programas que residen en una computadora o en un equipo especializado y que permiten controlan el tráfico de información entre varias redes. Tradicionalmente protegen la red interna de una entidad del acceso indebido de usuarios por medio de Internet.

**Gartner** - Serie de informes de investigación que muestra "fortalezas" y "advertencias" detalladas y las necesidades de tecnología. Tiene como objetivo proporcionar un análisis cualitativo, su dirección, madurez y participantes.

**Help Desk** - Personal que, en conjunto de recursos tecnológicos, presta servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias relacionadas a las Tecnologías de la Información y la Comunicación. Generalmente, el propósito es solucionar problemas o para orientar acerca de computadoras, equipos electrónicos o *software*.

**Imagen de computadora** - Proceso en que se instala a una (1) computadora el sistema operativo, los programas y las aplicaciones necesarias con sus licencias para que el suplidor replique estos programas en computadoras autorizadas.

**Integridad** - Es el proceso de proteger la información de alteraciones indebidas.

**IP Spoofing** - Uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

**Licencia para programas** - Es un contrato entre el autor del programa y el usuario, que permite utilizar el programa en forma legal. Las licencias contienen un acuerdo donde normalmente se estipula quiénes pueden utilizar el programa, los usos permitidos, si se pueden hacer copias del mismo, entre otras. Las compañías dedicadas a la venta de programación normalmente tienen disponibles diferentes tipos de licenciamiento, que se adaptan a las circunstancias y necesidades del cliente.

**Planeación de prevención de pérdidas**- Implica la calendarización de actividades tales como respaldo de sistemas, autenticación y autorización (seguridad), verificación de la presencia de virus y monitoreo de la utilización de los sistemas. Este último con el objetivo de verificar la capacidad y ejecutoria de los mismos.

**Programa** - Conjunto de instrucciones que permite que una computadora lleve a cabo una función. Los **programas de sistema** controlan el funcionamiento de las computadoras y las redes de informática. Los **programas de aplicación** facilitan y/o automatizan las operaciones que se realizan de forma manual, o que se lleven a cabo efectivamente.

**Recuperación de desastres** - Es la capacidad para responder a una interrupción de los servicios mediante la implementación de un plan para restablecer las funciones críticas de la organización.

**Remoción de contenido** - Proceso que elimina el contenido de los medios para almacenamiento de datos (discos duros, cintas magnéticas, memorias y otros), de tal manera que dicho contenido no pueda recuperarse en el futuro. Al momento existen diferentes métodos para la remoción de datos: *overwriting*, *degaussing* y la destrucción física del medio de almacenamiento.

1. **Degaussing** - Proceso en el que se utiliza un flujo magnético poderoso para eliminar los datos contenidos en un medio de almacenamiento magnético. Usualmente, el medio de almacenamiento queda inservible luego de este proceso.
2. **Overwriting** - Proceso en el que se reemplaza con nuevos datos los existentes en un medio electrónico de almacenamiento. Existen programas que hacen automáticamente este proceso por medio de la sobreescritura en patrones. Este método no se debe confundir con la reinicialización de discos (*format*) o eliminación de particiones del disco con la herramienta *fdisk*. El uso del *format* o el del *fdisk* no se consideran como métodos seguros de remoción de datos.

**Sistema de detección de intrusos** - Es un programa que reside en una computadora o en un equipo especializado para detectar ataques o intentos indebidos de acceso hacia un sistema de información.

**Seguridad de informática** - Protección de los sistemas de información en contra del acceso o la modificación física o electrónica no autorizada; de la información de protección en contra de la negación de servicios a usuarios autorizados o de la disponibilidad de servicios a usuarios no autorizados; las políticas, las normas, las medidas, el proceso y las herramientas necesarias para detectar, documentar, prevenir y contrarrestar los ataques a la información o servicios antes descritos; los procesos y herramientas necesarias para la restauración de la información o los sistemas afectados por las brechas en la seguridad, disponibilidad y protección de los recursos requeridos para establecer dicha seguridad.

**SLA (*Service Level Agreement*)** - Contrato en que se estipulan los niveles de un servicio en función de una serie de parámetros objetivos, establecidos de mutuo acuerdo entre ambas partes. Este puede incluir, pero no limitarse a, el nivel operativo de funcionamiento, las penalidades por caída de servicio y el tiempo de respuesta, entre otros.

**Spyware** - Es un programa que se instala inadvertidamente en una computadora y se propaga sin autorización a la información sobre el usuario y sus hábitos de utilización de Internet.

**Troyan** - Programas que se introducen en el ordenador por diversos medios, se instalan de forma permanente y por el cual tratan de tomar el control del sistema afectado. Llegan por medio de un programa aparentemente inofensivo que al ejecutarse instala el troyano. Aunque no suelen ser virus destructivos, pueden capturar datos personales y enviarlos al atacante o abrir brechas de seguridad para que este pueda tomar el control de la máquina de forma remota

**Usuario** - Persona que utiliza una computadora personal, tableta o portátil para realizar múltiples operaciones con aplicaciones, sistemas o plataformas.

**Virus** - *Malware* que tiene por objeto alterar el funcionamiento normal del ordenador, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos que solo se caracterizan por ser molestos.

**VPN (*Virtual Private Network*)** - tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

**Ventana de mantenimiento** - periodo de inactividad en que se realizan los trabajos de mantenimiento para que no afecten a la ejecución de flujos de trabajo. La ventana de

mantenimiento se anuncia previamente y se coordina el tiempo para las tareas de mantenimiento necesarias, tales como actualizaciones de *software*, *hardware*, actualizaciones de contraseñas, cargas especiales de datos y pruebas de los procedimientos de recuperación ante desastres, entre otros.

**Worm (Write Once Read Many)** - virus que se replica a sí mismo, pero no altera ningún archivo en su máquina. Sin embargo, pueden causar estragos al multiplicarse tantas veces que ocupan toda la memoria disponible del ordenador o el espacio en un disco duro.

**Zero Day** - defecto en el *software*, *hardware* o *firmware* que explota tan pronto sea descubierta por el público.

## **Referencias**

Seguridad de los Sistemas de Información Ley de Gobierno Electrónico, Política Núm.: TIG-003, Núm. 151 de 22 de junio de 2004.

Reglamento de Propiedad Excedente Estatal de la ASG, Reglamento Núm. 5064 de 2 de mayo de 1994, <http://www.gobierno.pr/ASG/reglamentos>.

Reglamento para Enmendar el Reglamento de Propiedad Excedente Estatal de la ASG Reglamento Núm. 6179 de 1 de agosto de 2000, <http://www.gobierno.pr/ASG/reglamentos>.

Política de Seguridad DE (2010).

Política sobre la adquisición y desarrollo de sistemas, equipo tecnológico y el uso de la tecnología informática en el DE. Carta Circular Núm. 7-2011-2012.

Anejo -04



20 de enero de 2015

**A Todo el Personal**

Prof. Rafael Roman Meléndez  
Secretario

### PROCEDIMIENTO PARA DAR DE BAJA A USUARIOS EN LOS SISTEMAS DE INFORMACIÓN

La Oficina de Sistemas de Información y Apoyo Tecnológico a la Docencia (OSIATD) es la unidad encargada de la planificación, implantación y mantenimiento de los sistemas de información utilizados en el Departamento de Educación (DE). OSIATD es responsable de crear las cuentas que dan acceso a estos sistemas en la red, de acuerdo con las funciones de los usuarios y aprobados por el supervisor inmediato, excepto las cuentas de los sistemas SIFDE y SIE, que administran la seguridad de las mismas. No obstante, OSIATD es responsable de velar por la seguridad de los todos los sistemas de información del DE.

Cuando un empleado cambia de funciones o deja de ser empleado del Departamento, por razón de licencia, renuncia, despido, jubilación o muerte, se identificará en el sistema STAFF por personal autorizado. La Oficina de la Secretaría Auxiliar de Recursos Humanos enviará un informe diariamente a la OSIATD para deshabilitar la cuenta de acceso a la red, de acuerdo con el Procedimiento de Políticas y Procedimientos de Seguridad. OSIATD enviará este informe a los administradores de SIFDE y SIE para que deshabiliten las cuentas correspondientes en sus sistemas e informen cuando completen el proceso. Con esta acción los accesos a todos los sistemas quedan inactivos.

De identificar alguna situación que amerite alguna acción inmediata en relación con la seguridad y el acceso a los sistemas de información, debe informarlo a OSIATD al 787 773 3076 o al correo electrónico [helpdesk@de.gobierno.pr](mailto:helpdesk@de.gobierno.pr). OSIATD procederá a verificar, tomar acción o canalizar la situación a la unidad correspondiente.

Este procedimiento entra en vigor a partir de su publicación.

Agradecemos la cooperación de todos para cumplir con este proceso y velar por la seguridad de los sistemas y datos del Departamento de Educación.

P.O. Box 190759  
San Juan, Puerto Rico 00919-0759  
Tel.: 787 773 2696  
[www.de.gobierno.pr](http://www.de.gobierno.pr)



El Departamento de Educación no discrimina de ninguna manera por razón de edad, raza, color, sexo, nacimiento, condición de veterano, ideología política o religiosa, origen o condición social, orientación sexual o identidad de género, discapacidad o impedimento físico o mental; ni por ser víctima de violencia doméstica, agresión sexual o acoso.

**Estado Libre Asociado de Puerto Rico  
Departamento de Educación  
Centro de Cómputos  
Formulario para Autorización de Cuenta de Usuario**

Rev 1.3.6 2015-4-8

**Información del Usuario:**

¿Tiene cuenta de usuario? (Si / No) De contestar **Sí** indique su cuenta de usuario: \_\_\_\_\_

Apellidos: \_\_\_\_\_ Nombre: \_\_\_\_\_ Inicial: \_\_\_\_\_

Teléfono y extensión: \_\_\_\_\_ Número TAL (Kronos): \_\_\_\_\_

Puesto: \_\_\_\_\_ Oficina y Localización: \_\_\_\_\_

**Clasificación del Empleado:**

- No Docente       Contrato de Servicios Personales o Profesionales y Consultivos       Genérico  
 Transitorio       Jornada Parcial       Temporero

Fecha de inicio: \_\_\_\_\_ Fecha de terminación: \_\_\_\_\_

**Acceso que solicita – Algunas de los accesos podrían requerir formulario y aprobación adicional.**

Aplicación	Marque [X]	Dueño de la Aplicación	Formulario Adicional
Enteract (Manejo y Rastreo de Documentos)		Centro de Cómputos	N/A
Staff		Recursos Humanos	Permisos deben ser autorizados por la oficina central de Recursos Humanos.
Internet		<b>El supervisor deberá escribir SI o NO y confirmar con sus iniciales</b> Si ___ No ___ Iniciales _____	
Correo Electrónico		<b>El supervisor deberá escribir SI o NO y confirmar con sus iniciales</b> Si ___ No ___ Iniciales _____	
Acceso VPN		<b>El supervisor deberá incluir carta justificativa para ésta solicitud.</b>	
Permiso Administrador Servidor		<b>El supervisor deberá incluir carta justificativa para ésta solicitud.</b>	

**Acuerdo de confidencialidad y responsabilidad:**

Acuerdo proteger la información del Departamento de Educación contenida en medios electrónicos e impresos o cualquier otro medio implícito o explícito donde pueda estar almacenada. La información a la que tengo acceso es para uso exclusivo de las funciones del puesto que ocupo y será utilizada única y exclusivamente para uso oficial. El código de acceso (cuenta de usuario y contraseña) es personal, confidencial e intransferible. No instalaré programa ni accederé a ninguna aplicación que no esté respaldada con la correspondiente autorización. No existe implícita o explícitamente expectativa de privacidad personal en la información almacenada en la máquina bajo mi responsabilidad propiedad del Estado Libre Asociado de Puerto Rico. La información contenida en dicha máquina está sujeta a supervisión y auditorias. La custodia de la máquina y el código de acceso lo acepto con pleno conocimiento de la responsabilidad que conlleva.

Firma de usuario: \_\_\_\_\_ Letra Molde \_\_\_\_\_

Firma del supervisor: \_\_\_\_\_ Letra Molde \_\_\_\_\_

**Para uso oficial:**

Cuenta de Usuario: \_\_\_\_\_ Fecha: \_\_\_\_\_

Asignado por: \_\_\_\_\_ Número Control: \_\_\_\_\_

**Guías para definir su contraseña:**

- Debe ser de seis o más caracteres, en combinación de números, letras mayúsculas, minúsculas y caracteres especiales.  
Ejemplo: Z54w&7\*k
- El sistema le solicitará cambiar la contraseña cada 60 días.
- La cuenta de usuario se definirá en no más de dos días laborables a partir del recibo del formulario.



**ESTADO LIBRE ASOCIADO DE PUERTO RICO**  
**DEPARTAMENTO DE EDUCACIÓN**

**OFICINA DE SISTEMAS DE INFORMACIÓN  
Y APOYO TECNOLÓGICO A LA DOCENCIA**

**Políticas para la Administración del Sistema de Información Estudiantil (SIE)**

1. El Sistema de Información Estudiantil (SIE) provee acceso a los usuarios de forma continua, 24 horas los 7 días de la semana. El Sistema no estará disponible en los momentos en que se esté realizando labores de actualización o mantenimiento.
2. Toda solicitud de servicio (creación de cuentas, reactivación de cuentas, cambio de contraseña, movimiento de empleados y deshabilitación de cuentas) debe realizarse a través de los formularios desarrollados para estos fines. Estos son:
  - Autorización para Cuenta de Usuario en SIE (SIE-F01)
  - Solicitud para Reactivar Cuentas de Usuarios – Sistema de Información Estudiantil (SIE-F02)
  - Solicitud de Cambio de Contraseña – Sistema de Información Estudiantil (SIE-F03)
  - Solicitud de Movimiento de Empleados (SIE-F04)
  - Solicitud para Deshabilitar Cuentas en los Sistemas de Información (OSIATD-F06)
3. Toda solicitud de servicio debe estar autorizada por el supervisor inmediato del solicitante.
4. Las solicitudes de servicios se deben entregar en las Oficinas de Sistema de Información y Apoyo Tecnológico a la Docencia (OSIATD), en el 4to piso de la antigua sede del Departamento de Educación (DE). Las mismas se pueden entregar personalmente o se puede enviar por correo electrónico a [de.sie@de.pr.gov](mailto:de.sie@de.pr.gov) o por fax al 787-767-6935.
5. La Oficina del Sistema de Información Estudiantil tendrá un periodo de no más de 15 días para atender cualquier solicitud de servicio. No obstante, durante los meses de mayor demanda, este periodo podría extenderse hasta 30 días. Este periodo aplicará únicamente a aquellas solicitudes cuyos formularios estén debidamente completados.
6. En los casos en los que se solicite un servicio, utilizando un formulario que no corresponde al servicio solicitado, se le notificará al solicitante para que proceda a llenar el formulario correcto.
7. Toda notificación al solicitante, se enviará a través del correo electrónico que éste incluya en la solicitud.
8. Las solicitudes trabajadas, deberán ser archivados por Región Escolar.

P.O.BOX 190759, SAN JUAN, PUERTO RICO 00919-0759 TEL: (787)773-2696 FAX: (787) 767-6935

El Departamento de Educación no discrimina por razón de raza, color, sexo, nacimiento, origen nacional, condición social, ideas políticas o religiosas, edad o impedimento en sus actividades, servicios educativos y oportunidades de empleo.

**Políticas para la Administración del Sistema de Información Estudiantil (SIE)**

Página 2

**A. Creación de Cuentas de Usuarios**

1. Las solicitudes para la creación de cuentas de usuarios serán trabajadas únicamente por el personal de la Oficina del SIE.
2. Para solicitar la creación de una nueva cuenta, el solicitante debe completar el formulario SIE-F01, denominado Autorización para Crear Cuenta de Usuario en SIE.
3. Todo empleado debe tener un número de empleado asignado por el Sistema de Tiempo, Asistencia y Licencia (TAL) de Kronos, para poder solicitar la creación de una cuenta.
4. Los usuarios que no tengan número de empleado, ya sea porque son transitorios o por contrato, deben acompañar la solicitud con evidencia que demuestre las funciones que están ejerciendo en la escuela o área de trabajo.
5. Todas las solicitudes recibidas, se deben registrar en la hoja de registro desarrollada para mantener un control de las mismas.
6. Antes de crear una cuenta, el personal del SIE debe asegurarse de:
  - a. Verificar en el Sistema (SIE) si el solicitante tiene o no cuenta creada.
  - b. Validar contra el Sistema de Recursos Humanos (STAFF), que el solicitante está registrado como empleado del DE y que el supervisor que autoriza la solicitud sea quien realmente supervisa al solicitante.
7. En los casos en que el solicitante tenga una cuenta creada, se le notificará a través del correo electrónico provisto por éste en la solicitud, que ya tiene cuenta creada. Como parte de la notificación, se orientará al solicitante para que proceda a solicitar la reactivación de su cuenta.

**B. Reactivación de Cuentas de Usuarios**

1. Las solicitudes para la reactivar cuentas de usuarios serán trabajadas únicamente por el personal de la Oficina del SIE.
2. Para solicitar la reactivación de una cuenta, el solicitante debe completar el formulario SIE-F02 denominado Solicitud Para Reactivar Cuentas de Usuarios – Sistema de Información Estudiantil.
3. Antes de reactivar una cuenta, se debe validar contra el Sistema de Recursos Humanos (STAFF), que el solicitante está registrado como empleado activo del DE.
4. Todas las solicitudes recibidas, se deben registrar en la hoja de registro desarrollada para mantener un control de las mismas.

**Políticas para la Administración del Sistema de Información Estudiantil (SIE)**

Página 3

**C. Cambio de Contraseña**

1. Las solicitudes para realizar cambios de contraseña serán trabajadas por los Directores Escolares y/o los Maestros Especialistas en Tecnología Educativa.
2. Para solicitar el cambio de contraseña, el solicitante debe completar el formulario SIE-F03 denominado Solicitud de Cambio de Contraseña – Sistema de Información Estudiantil. Bajo ningún concepto se podrá realizar un cambio de contraseña, si el solicitante no hace entrega de dicha solicitud.
3. Tanto el Director Escolar, como el Maestro Especialista que realice un cambio de contraseña, deberá orientar al solicitante para que proceda a cambiar la contraseña provisional que se le entregó, inmediatamente en su primer acceso al Sistema.
4. El Director Escolar y el Maestro Especialista deberán conservar y archivar todas las solicitudes trabajadas y tenerlas disponibles en el momento en que les sean requeridas. Las mismas deberán ser agrupadas por región.

**D. Movimiento de Empleados**

1. Las solicitudes para realizar movimiento de empleados en el SIE podrán ser atendidas por los Maestros Especialistas en Tecnología Educativa cuando se trate de maestros, directores, oficinistas y personal de disciplina. En el caso de los Maestros Especialistas en Tecnología Educativa Enlaces, estos también podrán atender las solicitudes relacionadas con el movimiento del resto de los Maestros Especialistas. No obstante, aquellas solicitudes relacionadas con el movimiento de personal de los otros programas en el DE, serán atendidas únicamente por el personal de la Oficina del SIE.
2. Para solicitar el cambio o movimiento de empleados dentro del SIE, el solicitante debe completar el formulario SIE-F04 denominado Solicitud de Movimiento de Empleados.
3. Los Maestros Especialistas en Tecnología Educativa y los Maestros Especialistas en Tecnología Educativa Enlaces, deberán enviar mensualmente a las Oficinas del SIE un informe de las solicitudes trabajadas, junto con las solicitudes trabajadas durante el respectivo mes. Las solicitudes deberán estar agrupadas por región.

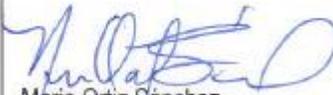
**E. Deshabilitación de Cuentas**

1. Las solicitudes para la deshabilitar cuentas de usuarios en el SIE, se atenderán únicamente por el personal de la Oficina del SIE.
2. Para solicitar la deshabilitación de una cuenta, el solicitante debe completar el formulario OSIATD-F06 denominado Solicitud para Deshabilitar Cuentas en los Sistemas de Información, y seleccionar el SIE dentro de las opciones que provee la solicitud.
3. Será responsabilidad de todo supervisor el solicitar la deshabilitación de una cuenta cuando un empleado a su cargo ha cambiado de funciones, se ha acogido a una licencia por más de tres meses, ha renunciado, se ha jubilado o cuando ha sido separado de su empleo.

Políticas para la Administración del Sistema de Información Estudiantil (SIE)

Página 4

4. La solicitud para la desactivación de una cuenta, se debe enviar con por lo menos catorce (14) días de antelación a la efectividad del cambio.

Sometido por:	Aprobado por:
 <u>Marie Ortiz Sanchez</u> Directora Ejecutiva III	 <u>Ing. Maribel Picó Piereschi</u> Principal Oficial de Informática
<u>3/25/2013</u> Fecha	

**Estado Libre Asociado de Puerto Rico**  
**Departamento de Educación**  
**Oficina de Sistemas de Información y Apoyo Tecnológico a la Docencia (OSIATD)**  
SIE-F01 Rev. marzo 2013

**SOLICITUD DE AUTORIZACIÓN PARA CREAR CUENTA DE USUARIO EN SIE**

**I. Información del Empleado:**

Apellidos: \_\_\_\_\_ Nombre: \_\_\_\_\_  
Seguro Social: \_\_\_\_\_ Teléfono y extensión y/o celular: \_\_\_\_\_  
Puesto: \_\_\_\_\_ Escuela y Código: \_\_\_\_\_  
Número de Empleado: \_\_\_\_\_ Distrito: \_\_\_\_\_  
Correo Electrónico: \_\_\_\_\_

**II. Acceso a SchoolMAX®:** (Se requiere aprobación del Director(a) o Supervisor(a) del Área)

Rol a desarrollar en SchoolMAX®:

Director(a) de Escuela (All Admin)       Estadístico(a)       Consejero(a) o Trabajador(a) Social  
 Secretaria Escolar (All Admin)       Registrador(a)       Especialista en Tecnología  
 Asistencia – Administrativo       Maestro(a)       Otro: \_\_\_\_\_

**III. Acuerdo de Confidencialidad:** (lea cuidadosamente y firme)

Al tener acceso al Sistema de Información Estudiantil (SchoolMAX®), entiendo que podre acceder información confidencial de estudiantes, familias y personal y por ello me comprometo a:

- **Proteger la información disponible en el SIE de acuerdo y en cumplimiento con las leyes y reglamentos aplicables, tanto a nivel estatal como federal.**
- **No discutir la información con personal no autorizado.**
- **No permitir que el personal no autorizado pueda ver los archivos.**
- **No compartir con nadie mi código de acceso (Username) y contraseña (Password).**
- **Seguir y cumplir con la Política sobre el Uso Aceptable del Internet del Departamento de Educación de Puerto Rico, disponibles en el portal electrónico del DEPR [www.de.gobierno.pr](http://www.de.gobierno.pr).**

Entiendo que de no cumplir o violar el acuerdo descrito arriba puede resultar en acciones disciplinarias según descritas en el Manual sobre Políticas de Uso Aceptable del Internet del Departamento de Educación de Puerto Rico. La violación de este acuerdo también puede conllevar violaciones de leyes estatales y federales por lo que puede aplicarse responsabilidad legal y penalidades.

Firma: \_\_\_\_\_ Fecha: \_\_\_\_\_

**IV. Acuerdo de No-Divulgación:** (lea cuidadosamente y firme)

Acuerdo proteger la información del DEPR (incluyendo toda la información conservada en medio electrónicos portátiles y también en formato impreso) usando mi cuenta autorizada, protegiendo la información que manejo con mi mejor habilidad y esfuerzo. No permitiré que otra persona del DEPR o fuera use mi cuenta personal o conozca mi contraseña. Entiendo que si no cumplo con este acuerdo resultara en acciones disciplinarias incluyendo la terminación de la cuenta por tiempo indefinido. No copiaré o instalaré ningún programa ilegal o no autorizado por OSIATD en la red o en las computadoras personales. Usaré mi cuenta solo para actividades de trabajo del DEPR. Soy responsable por todas las acciones realizadas con mi cuenta incluyendo el acceso de páginas de Internet indebidas, según las políticas del DEPR. Informaré a OSIATD si sospecho del uso no autorizado de mi cuenta.

Firma: \_\_\_\_\_ Fecha: \_\_\_\_\_

**V. Autorización del Director(a) o Supervisor(a) de Área:**

Esta cuenta es requerida para cumplir con los objetivos del Departamento por lo cual autorizo la misma. Estoy de acuerdo en notificar si la persona para la cual se crea esta cuenta, termina sus funciones para el DEPR o es trasladada a otra Área del DEPR. El (la) Director(a) o Supervisor(a) de Área conservará una copia de este formulario para su récord.

Firma del Director(a) o Supervisor(a) de Área      Nombre en letra de molde      Fecha

**ATENCIÓN:** Solo se crearán cuentas por medio de este formulario. El formulario debe estar lleno en su totalidad y firmado por el personal autorizado. Envíe este formulario por fax al (787) 767-6935. **No utilice este formulario para solicitar cambio de contraseña y/o cambio de escuela.**

**Para uso del personal de OSIATD**

Cuenta del Usuario (Username) Asignado: \_\_\_\_\_ Rol: \_\_\_\_\_

Asignado por: \_\_\_\_\_ Fecha: \_\_\_\_\_ Núm. de Referencia: \_\_\_\_\_



**ESTADO LIBRE ASOCIADO DE PUERTO RICO  
DEPARTAMENTO DE EDUCACIÓN**

**OFICINA DE SISTEMAS DE INFORMACIÓN  
Y APOYO TECNOLÓGICO A LA DOCENCIA**

**Políticas para la Creación de Cuentas de Usuarios para el Portal de Padres  
Sistema de Información Estudiantil (SIE)**

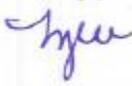
1. El acceso al Portal de Padres es de forma continua, 24 horas los 7 días de la semana. El Sistema no estará disponible en los momentos en que se esté realizando labores de actualización o mantenimiento.
2. El proceso de creación de cuentas de padres iniciará una vez el Director complete el 85% de la organización escolar de su escuela en el SIE.
3. El Sistema asignará a cada padre<sup>1</sup>, tutor o encargado una clave de acceso, la cuál debe ser utilizada por éste para crear su cuenta.
4. Los Directores Escolares deben imprimir y mantener para su uso la lista de los padres, tutores o encargados de los estudiantes asignados a su escuela con la clave de acceso que le fue asignada a cada uno por el Sistema.
5. Para tener acceso al Portal, el padre, tutor o encargado del estudiante debe visitar la escuela para obtener la clave de acceso que le permitirá crear su cuenta de usuario.
6. Antes de hacer entrega al padre, tutor o encargado de la clave de acceso asignada por el Sistema, el Director Escolar debe asegurarse de que éste no tenga ya una cuenta creada para cualquiera de sus hijos. Solamente hará entrega de la clave de acceso a aquellos padres, tutores o encargados que no tengan cuentas creadas.
7. Todo padre, tutor o encargado debe llenar el formulario SIE-F05, Acuerdo y Políticas de Uso para Cuentas de Padres (APU), al inicio de cada curso escolar. Es importante que el Director le recalque que al firmar el documento, éste se compromete a darle el debido uso al Sistema, a proteger la información de los estudiantes, a no compartir su cuenta de usuario con nadie y a proteger su contraseña. Se compromete además a mantener actualizada la información de contacto del grupo familiar. La firma de este acuerdo es requisito para tener una cuenta de acceso al Portal de Padres. El Director entregará una copia del documento firmado al padre, tutor o encargado.

<sup>1</sup> El término padre se refiere a ambos géneros (padre y madre).

**Políticas para las Creación de Cuentas de Usuarios para el Portal de Padres Sistema de Información Estudiantil (SIE)**

Página 2

8. Los Directores Escolares deben solicitar una identificación con foto como método de validación de identidad, antes de entregar la clave de acceso.
9. Los Directores Escolares proveerá una orientación básica sobre la utilización del Portal.
10. Cuando el padre, tutor o encargado confronte alguna situación con el proceso para crear su cuenta, debe notificar al Director Escolar. Si el Director Escolar no logra resolver la situación, éste se comunicará con el Maestro Especialista en Tecnología Educativa.

Sometido por:	Aprobado por:
 <u>Marie Ortiz Sánchez</u> Directora Ejecutiva III	 <u>Ing. Maribel Picó Piereschi</u> Principal Oficial de Informática
<u>3/25/2013</u> Fecha	